

2/5/1

DIALOG(R)File 351:Derwent WPI  
(c) 2004 Thomson Derwent. All rts. reserv.

012628490      \*\*Image available\*\*

WPI Acc No: 1999-434594/ 199937

XRPX Acc No: N99-323923

Document existence certification method in computer network - involves  
transmitting hash URL to registrant terminal, after acquiring document  
using server

Patent Assignee: HITACHI LTD (HITA )

Number of Countries: 001 Number of Patents: 001

Patent Family:

| Patent No   | Kind | Date     | Applicat No | Kind | Date     | Week     |
|-------------|------|----------|-------------|------|----------|----------|
| JP 11175512 | A    | 19990702 | JP 97338364 | A    | 19971209 | 199937 B |

Priority Applications (No Type Date): JP 97338364 A 19971209

Patent Details:

| Patent No   | Kind | Lan Pg | Main IPC    | Filing Notes |
|-------------|------|--------|-------------|--------------|
| JP 11175512 | A    | 11     | G06F-017/21 |              |

Abstract (Basic): JP 11175512 A

NOVELTY - A server (1) acquires a document (11) using designated URL, after receiving registration demand of existence proof information from registrant terminal (3). A hash (14) is generated from registration date, document URL and the document and their link is registered in a database (13). The hash URL is then transmitted to registrant terminal.

USE - For document existence certification in client server network.

ADVANTAGE - Duplication object of document can be preserved locally and reliability of truth or falsehood can be given to other perusal person. DESCRIPTION OF DRAWING(S) - The figure shows systematic diagram of certification system. (1) Server; (3) Registrant terminal; (11) Document; (13) Database; (14) Hash.

Dwg.1/12

Title Terms: DOCUMENT; EXIST; CERTIFY; METHOD; COMPUTER; NETWORK; TRANSMIT; HASH; TERMINAL; AFTER; ACQUIRE; DOCUMENT; SERVE

Derwent Class: P85; T01

International Patent Class (Main): G06F-017/21

International Patent Class (Additional): G06F-015/00; G09C-001/00

File Segment: EPI; EngPI

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-175512

(43) 公開日 平成11年(1999) 7月2日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 0 6 F 17/21

15/00

3 1 0

// G 0 9 C 1/00

6 4 0

G 0 6 F 15/20

15/00

5 9 0 Z

3 1 0 A

G 0 9 C 1/00

6 4 0 Z

G 0 6 F 15/20

5 7 0 R

審査請求 未請求 請求項の数 3 O L (全 11 頁)

(21) 出願番号

特願平9-338364

(22) 出願日

平成9年(1997)12月9日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 森田 光

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所ビジネスシステム開発  
センタ内

(72) 発明者 千葉 寛之

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所ビジネスシステム開発  
センタ内

(74) 代理人 弁理士 高橋 明夫 (外1名)

最終頁に続く

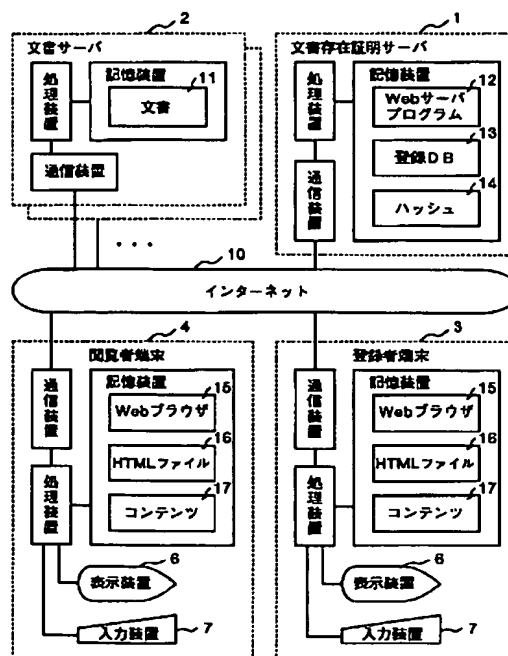
(54) 【発明の名称】 文書存在証明に関するプログラム

(57) 【要約】

【課題】 オリジナル文書が特定の日付に特定の格納場所存在したことを証明する。

【解決手段】 登録者端末3は、文書11の複製物をコンテンツ17として保存する。登録者端末3からの存在証明情報の登録要求に応答して文書存在証明サーバ1は、指定されたURLによって文書11を取得し、登録日付、文書URL及び文書11の内容からハッシュ14を生成し、そのリンクを登録DB13に登録し、登録者端末3へハッシュURLを通知する。登録者端末3はハッシュURLを含む存在確認ページを作成してHTMLファイル16に保存する。コンテンツ17及びHTMLファイル16の複製物を取得した閲覧者端末4は、コンテンツ及び存在確認ページ中の登録日付、文書URLに基づいてハッシュを生成し、文書存在証明サーバ1から取得したハッシュ14と比較してオリジナル文書の存在を検証する。

図 1



## 【特許請求の範囲】

【請求項 1】コンピュータ読み取り可能な記憶媒体に実体化されたコンピュータプログラムであり、特定の文書が特定の日付に特定の格納場所に存在したことを証明するクライアント計算機の支援をするサーバ計算機によって実行されるプログラムであって、該プログラムは下記のステップを含む：

(a) クライアント計算機からの文書の存在証明情報の登録要求に回答して指定された文書の格納場所から該文書のオリジナルを取得し、(b) 該文書のコンテンツ、該文書の格納場所及び登録日付を含む情報から縮小された代替情報を生成し、(c) 該代替情報を記憶装置に保存し、(d) クライアント計算機が該代替情報に基づいて該文書の存在証明を実施可能のようにクライアント計算機へ該代替情報の格納場所を通知する。

【請求項 2】コンピュータ読み取り可能な記憶媒体に実体化されたコンピュータプログラムであり、特定の文書が特定の日付に特定の格納場所に存在したことを証明するクライアント計算機と該文書のオリジナルのコンテンツ、該文書の格納場所及び登録日付を含む情報から生成された縮小された代替情報を登録するサーバ計算機とを有するシステムのうち、該クライアント計算機によって実行されるプログラムであって、該プログラムは下記のステップを含む：

(a) 該文書の複製物のコンテンツ、該文書の格納場所及び登録日付から縮小された代替情報を生成し、(b) 該サーバ計算機から取得した対応する代替情報と生成した代替情報とが一致することによって該文書の存在証明をする。

【請求項 3】該プログラムは、さらに上記 (a) 及び (b) のステップの前に、該サーバ計算機へ該文書の格納場所を送信して該代替情報の登録要求を行い、該代替情報の格納場所を受信するステップを含むことを特徴とする請求項 2 記載のコンピュータプログラム。

## 【発明の詳細な説明】

## 【0001】

【本発明の属する技術分野】本発明は、ネットワーク上に存在する文書が特定の日付に特定の格納場所に存在したことを証明する技術に係わり、特に文書の存在証明を支援するサーバ計算機に登録された存在証明情報を利用して文書の存在証明を行う方法に関する。

## 【0002】

【従来の技術】World Wide Webを用いることによって、ネットワーク上に分散したサーバが格納する文書をWebページの形式で不特定多数のクライアントに公開し、さらに他の文書の参照を行うために他の文書の格納場所を示すリンクを文書中に埋め込むことによってクライアントはネットワーク上に分散する数多くの文書を効率良く閲覧することが可能となる。

【0003】しかし各サーバの管理者もしくは各文書の

提供者が異なるため、文書によってはリンク先のWebページなどの文書が変更されたり消滅する可能性がある。そのためその文書の改変もしくは消滅などといった事態を回避する手段の一つとして、各個人が個別に特定の文書の複製物を保存することが挙げられる。この場合、このようにして保存された文書のオリジナルが元々のリンク先によって示される格納場所にローカルに保存された通りの内容で存在したものか否かを証明する手段は存在しない。

## 10 【0004】

【発明が解決しようとする課題】以上述べたように、リンク先のWebページなどの文書の変更や消滅などに対処するためには、その文書を利用しようとする者が個別に保存することが考えられるが、このようにして保存された文書のオリジナルが元々の格納場所によって同定される場所に存在したものか否かを証明する手段は存在せず、この文書の複製物を個別に保存した者がこの複製物を他者に提供する際に、この文書のオリジナルの発信源を証明することができないという問題があった。

20 【0005】本発明は上記事情に鑑みてなされたものであり、その目的とするところは、特定の文書が特定の日付に特定の格納場所に存在したことを示す存在証明情報を登録する手段を提供することにあり、またこの存在証明情報を利用して文書の存在証明をする手段を提供することにある。

## 【0006】

【課題を解決するための手段】本発明に関する情報システムは、文書の存在証明情報の登録を要求する登録者のクライアント計算機、この登録要求に回答して文書の存在証明情報を登録するサーバ計算機及び文書の複製物の提供を受け元々の文書の存在証明をする閲覧者のクライアント計算機を有する。サーバ計算機で実行されるプログラムは、クライアント計算機からの文書の存在証明情報の登録要求に回答して指定された文書の格納場所からこの文書のオリジナルを取得し、文書のコンテンツ、文書の格納場所及び登録日付を含む情報から縮小された代替情報を生成し、この代替情報を記憶装置に保存し、クライアント計算機がこの代替情報に基づいてオリジナル文書の存在証明を実施可能のようにクライアント計算機へ代替情報の格納場所を通知する。また閲覧者のクライアント計算機で実行されるプログラムは、文書の複製物のコンテンツ、文書の格納場所及び登録日付から縮小された代替情報を生成し、サーバ計算機から取得した対応する代替情報と生成した代替情報とが一致するのを確認することによってオリジナル文書の存在証明をする。

40 【0007】本発明によれば、登録日付以後にオリジナル文書が改変されたか消滅したかに関わらず元々の文書の存在を証明することができる。

## 【0008】

50 【発明の実施の形態】以下本発明の一実施形態について

## 3

図面を用いて詳細に説明する。

【0009】図1は、World Wide Webに関するシステム構成を示す構成図である。文書サーバ2は処理装置、記憶装置及びインターネット10に接続するための通信装置を含む計算機であり、その記憶装置には元々の提供者から提供された文書11のオリジナルを格納する。文書存在証明サーバ1は、公に認められた第3者機関のサーバであり、同様に処理装置、記憶装置及び通信装置を含む計算機であり、その記憶装置にはWebサーバプログラム12、登録データベース(DB)13及びハッシュ14を格納する。ハッシュ14は文書11のコンテンツ等から計算されるハッシュである。登録DB13は、文書11の存在証明情報の一部を格納する。この存在証明情報は、登録日付、文書11のUniform Resource Locator (以下URLと略す)、ハッシュ14のURL等を含む。Webサーバプログラム12は、従来のWebサーバプログラムの機能のほかに登録者端末3からの要求に従って文書11のコンテンツ等からハッシュ14を計算して記憶装置に格納するとともに存在証明情報を登録DB13に格納する。

【0010】登録者端末3は、処理装置、記憶装置、通信装置、表示装置6及び入力装置7を含むパソコンのようなクライアント計算機であり、その記憶装置にはWebブラウザ15、HTML(Hypertext Markup Language)ファイル16及びコンテンツ17を格納する。コンテンツ17は文書11の複製物としてローカルに保存されるものである。HTMLファイル16は文書11の存在確認をするための表示ページを格納するファイルである。Webブラウザ15は、従来のWebブラウザの機能のほかに文書存在証明サーバ1に文書11についての存在証明情報の登録を要求し、文書存在証明サーバ1に存在証明情報が登録されたとき文書11の存在確認をするための存在確認ページを生成してHTMLファイル16に格納するプログラムである。表示装置6はコンテンツ17、HTMLファイル16等を表示する装置であり、入力装置7はWebブラウザ15に対して登録等の指示をするキーボード、マウス等の入力装置である。

【0011】閲覧者端末4は、処理装置、記憶装置、通信装置、表示装置6及び入力装置7を含むパソコンのようなクライアント計算機であり、その記憶装置にはWebブラウザ15、HTMLファイル16及びコンテンツ17を格納する。コンテンツ17は登録者端末3のコンテンツ17の複製物として保存されるものである。HTMLファイル16は登録者端末3のHTMLファイル16の複製物として保存されるものである。Webブラウザ15は、従来のWebブラウザの機能のほかにコンテンツ17等からハッシュを計算し、HTMLファイル16中のハッシュURLに基づいて文書存在証明サーバ1

## 4

にアクセスしてハッシュ14を取得し、両ハッシュの一致を確認する検証処理を行うプログラムである。表示装置6はコンテンツ17、HTMLファイル16等を表示する装置であり、入力装置7はWebブラウザ15に対して検証等の指示をするキーボード、マウス等の入力装置である。

【0012】登録者端末3は、入力装置7からの指示に従って文書サーバ2にアクセスし、文書11の複製物を取得し、コンテンツ17として記憶装置に格納し、表示装置6上に表示する。入力装置7を介してこのコンテンツ17の存在証明情報の登録を要求されたとき、Webブラウザ15は、文書11のURLを文書存在証明サーバ1へ送信して登録要求を行う。文書存在証明サーバ1のWebサーバプログラム12はこの要求を受け取り、文書サーバ2にアクセスして文書11を取得し、登録日付、文書URL及び文書11のコンテンツからハッシュ14を計算して記憶装置に格納し、登録日付、文書URL及びハッシュURLを含む存在証明情報を作成して登録DB13に格納する。また登録者端末3にはハッシュURLを返送する。登録者端末3のWebブラウザ15は、登録日付、文書URL、コンテンツ17へのリンク及び受け取ったハッシュURLから成る存在確認ページを生成し、存在確認を検証してから存在確認ページをHTMLファイル16に格納する。閲覧者端末4のWebブラウザ15は、登録者端末3からコンテンツ17及びHTMLファイル16の複製物を取得してその記憶装置に格納する。入力装置7を介してコンテンツ17の存在確認の検証を要求されたとき、Webブラウザ15は、コンテンツ17、HTMLファイル16中の登録日付及び文書URLからハッシュを計算し、HTMLファイル16中のハッシュURLに基づいて文書存在証明サーバ1にアクセスしてハッシュ14を取得して両ハッシュが一致することを確認する検証処理を行う。

【0013】図2は、登録DB13のデータ構成を示す図である。登録DB13の各レコードは、登録日付、メールアドレス、文書URL及びハッシュURLから構成される。登録日付は本レコードの登録を行った日付、メールアドレスは登録者の電子メールアドレス、文書URLは存在証明する文書11の元の存在場所を示すURL、ハッシュURLはこの文書に関するハッシュ14を格納する文書存在証明サーバ1の格納場所を示すURLである。各レコードに登録者のメールアドレスを加える理由は、同一日に同一文書URLについて複数の登録者から登録要求があった場合に各登録者ごとのレコードを特定するためである。従ってメールアドレスの代わりにユーザIDなど登録者を識別する他の識別子を用いてもよい。

【0014】図3は、HTMLファイル16の内容を示す図である。HTMLファイル16は、HTMLで記述され、存在確認ページを表示するために使用され、登録

日付、コンテンツ17の元の存在場所を示すURL、当該登録者端末3が保有するコンテンツ17の格納場所（リンク）及び文書存在証明サーバ1に保存されたハッシュのURLを含む。コンテンツ17のリンクとは、登録者端末3のURLに特定のコンテンツ17の識別子を付加したものである。ハッシュのURLとは、文書存在証明サーバ1のURLに特定のハッシュの識別子を付加したものである。

【0015】図4は、登録者端末3のWebブラウザ15の処理の流れを示すフローチャートであり、特にハッシュを含む文書の存在証明情報を文書存在証明サーバ1に登録する処理の手順を示す。Webブラウザ15は、コンテンツ17を表示装置6上に表示し、入力装置7からコンテンツ17の存在証明情報の登録を指示されたとき、文書の元の存在場所を示すURLに電子署名を施した後、この電子署名を施した文書URLと登録者の電子メールアドレスを文書存在証明サーバ1へ送信し、登録要求を行う（ステップ21）。ここで電子署名を施すとは、RSA研究所の提唱するPKCS（Public Key Cryptography Standard）#7で定義される手法を用いて対象データに署名を施すことである。次に後で利用できるように当日の日付（グリニッジ標準時）、文書URL及び文書のコンテンツを登録者端末3の記憶装置に格納する（ステップ22）。文書存在証明サーバ1から登録情報を受信したとき（ステップ23）、その登録結果を調べて登録が行われたか否かを判定する（ステップ24）。登録が行われなかった場合（ステップ24No）、ステップ21に戻る。登録が行われた場合（ステップ24Yes）、記憶装置に格納された登録日付、文書URL及びステップ23で受信したハッシュURLを表示装置6に表示し、次いでこれにコンテンツ17へのリンクを加えた存在確認ページを生成して表示装置6に表示する（ステップ25）。入力装置7を介して検証が指示されたとき、記憶装置に格納した文書URL、コンテンツ及び登録日付をタプルとしてハッシュを計算する（ステップ26）。ここでハッシュの計算とは、例えば160ビットSHA-1ハッシュを求めると、すなわちHをハッシュ関数、tをタプルとするとH(t)を求めることである。ハッシュは文書URL、登録日付及び元の文書11の縮小された代替情報とみなせる。次にステップ23で登録情報として受信したハッシュURLにアクセスし、文書存在証明サーバ1に保存されたハッシュ14を取得する（ステップ27）。次に取得したハッシュに文書存在証明サーバ1の電子署名が施されているか否かを判定し、かつ取得したハッシュとステップ26で計算したハッシュとを比較して両者が一致するか否かを判定する（ステップ28）。ハッシュの電子署名とは、ハッシュが文書存在証明サーバ1の秘密鍵によって暗号化されたものであり、この暗号化されたハッシュを登録者端末3のもつ公開鍵

によって復号することによって文書存在証明サーバ1が認めたハッシュか否かを判定可能である。文書存在証明サーバ1の署名がないか両ハッシュが一致しない場合には（ステップ28No）、処理を中止する。文書存在証明サーバ1の署名があり両ハッシュが一致した場合には（ステップ28Yes）、生成した存在確認ページをHTMLファイル16として記憶装置に格納する（ステップ29）。ステップ25～28は、文書の存在証明情報が正しく文書存在証明サーバ1に登録されたことを検証する処理である。なおすでに文書存在証明サーバ1に登録された文書の存在証明情報を削除する場合には、登録日付、文書URL及びメールアドレスを文書存在証明サーバ1に送信し、削除要求を行えばよい。

【0016】図5は、文書存在証明サーバ1のWebサーバプログラム12の処理のうち、文書の存在証明情報を登録する処理の流れを示すフローチャートである。登録者端末3から登録要求又は削除要求を受信すると（ステップ31）、受信した文書URLに署名が施されているか否かを判定する（ステップ32）。署名が確認できない場合（ステップ32No）、記憶装置上の処理情報として登録結果（Result）に未登録、エラーコード（errorCode）に不正署名（invalid Signature）をセットし（ステップ33）、ステップ46へ行く。署名が施されている場合（ステップ32Yes）、要求が削除要求か否かを判定する（ステップ34）。削除要求であれば（ステップ34Yes）、後述の削除処理を行う（ステップ35）。登録要求であれば（ステップ34No）、文書11のコンテンツを取得するために受信した文書URLが指す文書サーバ2にアクセスする（ステップ36）。次に文書URLにアクセスできたか否かを判定する（ステップ37）。アクセスできなかった場合（ステップ37Yes）、記憶装置上のカウンタに1を加え（ステップ38）、カウンタの内容が所定値以下か否かを判定する（ステップ39）。所定値以下であれば（ステップ39Yes）ステップ36に戻って文書URLへのアクセスを再試行する。カウンタの内容が所定値を越えたとき（ステップ39No）、処理情報の登録結果に未登録、エラーコードに取得不能（Unreachable）をセットし（ステップ40）、ステップ46へ行く。文書サーバ2から文書11のコンテンツを取得したとき（ステップ37No）、取得したコンテンツを検索してこの文書を文書存在証明サーバ1に登録することに関して文書の提供者が同意する旨の署名があるか否かを判定する（ステップ41）。同意の署名がない場合には（ステップ41No）、処理情報の登録結果に未登録、エラーコードに提供者拒否（AuthorReject）をセットし（ステップ42）、ステップ46へ行く。同意の署名がある場合には（ステップ41Yes）、文書URL、取得したコンテンツ及び登録当日の日付からハッシュを計算

し、ハッシュに署名を施し（ステップ43）、署名とハッシュを記憶装置上のハッシュ14に格納し、登録DB13に登録レコードを追加する（ステップ44）。ハッシュの計算方式は、ステップ26の計算方式と同じである。登録する情報は、登録者端末3から受信したメールアドレス、文書URLと、登録日付、ハッシュ14の格納場所を示すハッシュURLである。次に処理情報の登録結果に登録済（OK）をセットし、ハッシュURLを付加する（ステップ45）。最後に登録情報として登録結果（登録済）とハッシュURL又は登録結果（未登録）とエラーコードを登録者端末3へ送信する（ステップ46）。なおWebサーバプログラム12は、登録者端末3又は閲覧者端末4からハッシュURLを指定したハッシュの要求があったとき、指定された格納場所からハッシュ14を取り出して送信する。

【0017】図6は、Webサーバプログラム12の処理のうち、文書の存在証明情報を削除する処理の流れを示すフローチャートである。Webサーバプログラム12は、登録者端末3から受信した登録日付、文書URLおよびメールアドレスをキーとして登録DB13を検索し（ステップ51）、該当するレコードが存在するか否かを判定する（ステップ52）。該当データが存在する場合には（ステップ52Yes）、該当するレコードのハッシュURLの指すハッシュ14及び登録DB13上の該当レコードを削除する（ステップ53）。次に記憶装置上の処理情報として削除結果に削除済（OK）をセットし（ステップ54）、削除結果を登録者端末3へ通知する（ステップ55）。該当データが存在しない場合には（ステップ52No）、処理情報の削除結果に未削除、エラーコードに「データが見当らない」（Data Not Found）をセットし（ステップ56）、ステップ55へ行く。ステップ55では削除結果とエラーコードを登録者端末3へ通知する。

【0018】文書の閲覧者によって操作される閲覧者端末4のWebブラウザ15は、登録者端末3からコンテンツ17を取得し、閲覧者端末4の記憶装置に格納し、表示装置6上に表示することが可能であり、閲覧者による文書の閲覧が可能である。以下閲覧者の必要性によってこの文書が元の存在場所に存在したことを検証するときの閲覧者端末4の検証処理について説明する。

【0019】図7は、閲覧者端末4のWebブラウザ15による検証処理の流れを示すフローチャートである。入力装置7からの指示に従ってWebブラウザ15は、登録者端末3にアクセスし存在確認ページを記述するHTMLファイル16を取得して表示装置6上に存在確認ページを表示する（ステップ61）。次に入力装置7を介して検証が指示されたとき、存在確認ページ中の文書URL、登録日付及びコンテンツ17をタプルとしてハッシュを計算する（ステップ62）。次に存在確認ページ中のハッシュURLにアクセスし、文書存在証明サ

バ1に保存されたハッシュを取得する（ステップ63）。次に取得したハッシュに文書存在証明サーバ1の電子署名が施されているか否かを判定し、かつ取得したハッシュとステップ62で計算したハッシュとを比較して両者が一致するか否かを判定する（ステップ64）。文書存在証明サーバ1の署名があり両ハッシュが一致した場合には（ステップ64Yes）、処理情報の処理結果を証明成功（OK）にセットする（ステップ65）。文書存在証明サーバ1の署名がないか両ハッシュが一致しない場合には（ステップ64No）、処理結果を証明失敗（Fail）にセットして（ステップ67）、ステップ66へ行く。最後に処理結果を表示装置6上に表示する（ステップ66）。

【0020】図8は、登録者端末3の表示装置6上に表示されたコンテンツ17を示す図である。入力装置7を介して「登録」ボタンが指示されると、Webブラウザ15はこのコンテンツ17の元の文書11の文書URLと登録者の電子メールアドレスを文書存在証明サーバ1へ送信し、文書11の存在証明情報を登録するよう要求する。

【0021】図9は、登録者端末3の表示装置6上に表示された登録情報を示す図である。登録日付及び文書URLは登録者端末3の記憶装置から取り出したもの、ハッシュへのリンクは文書存在証明サーバ1から受信したハッシュURLである。

【0022】図10は、登録者端末3の表示装置6に表示された存在確認ページを示す図である。コンテンツへのリンクは、コンテンツ17の格納場所を示す情報である。入力装置7を介して「検証」ボタンが指示されると、検証処理が開始される。また閲覧者端末4の表示装置6上にも閲覧者の指示によってこの存在確認ページが表示され、同様に「検証」ボタンの指示によって検証処理が開始される。

【0023】図11は、閲覧者端末4の表示装置6上に表示された文書の存在を証明するメッセージを示す図である。これによって閲覧者は、指定されたコンテンツ17の元の文書が登録日付で示される日に文書URLで示される格納場所に存在していたことを確認することができる。入力装置7を介してコンテンツへのリンクを指示すると、Webブラウザ15は記憶装置上のコンテンツ17を表示装置6上に表示し、図8に示す表示画面となる。

【0024】図12は、登録者端末3及び閲覧者端末4の表示装置6に表示された参考URLを示す図である。従来の論文において参考文献を提示するのと同様に、Webページに参考URLを添付することがある。この場合、リンク先の文書に変更があった場合には参考URLが意味をなさなくなる可能性がある。これを避けるために参考文書の複製物をコンテンツ17として登録者端末3に保存し、このコンテンツ17を他の閲覧者端末4に

提供することが考えられる。この場合、文書は参考URLで示される元々存在した場所以外の場所に保存されることになる。そこで閲覧者端末4にコンテンツ17だけでなくHTMLファイル16、すなわち存在確認ページも提供することにすれば、閲覧者は上記の検証処理を行うことによって参考URLで示される文書がその場所に存在していたことを確認することができる。図12に示す例は、各参考URLに「確認」としてコンテンツ17へのリンクと存在確認ページのURLを付加した例である。ここでコンテンツ17へのリンクは登録者端末3のURLに特定のコンテンツ17の識別子を付加したものであり、存在確認ページのURLは登録者端末3のURLに特定のHTMLファイル16の識別子を付加したものである。閲覧者端末4の入力装置7を介して「確認」が指示されたとき、Webブラウザ15は、図8に示すようなコンテンツとともに図10に示すような存在確認ページを表示装置6に表示するので、入力装置7を介して「検証」ボタンが指示されれば上記のような検証処理を実行する。

【0025】なお上記実施形態では文書URL、コンテンツ及び登録日付を代表する縮小された代替情報として計算によって求められたハッシュを挙げたが、上記の目的に沿うのであればハッシュの代わりに他の方式によって生成した代替情報であってもよい。また登録DB13に登録された各レコードに含まれる登録日付、メールアドレス及び文書URLは、レコードを削除するときの検索キーとして利用するほかに、登録日付の古い登録者に対して電子メールによって通知するなど登録DB13の管理のために使用される。登録DB13の管理は本発明と直接関係しないので、ハッシュURLによって特定の登録者の特定のハッシュ14にアクセスできるならば文書存在証明サーバ1に登録DB13を設けなくても本発明を実施できる。

#### 【0026】

【発明の効果】以上説明したように本発明によれば、サーバ計算機は登録日付に指定された文書の格納場所からオリジナル文書を引き出してこれら情報の縮小された代替情報を生成して登録するので、クライアント計算機に保存された登録日付、文書の格納場所及びローカルに保

存された文書の複製物から生成された代替情報とサーバに登録された代替情報とを比較することによって、ローカルに保存された文書の複製物がオリジナル文書と同じものであることを実証することができる。これによって他の閲覧者に対してローカルに保存された文書の複製物を提供するに際して、情報の信頼性や真贋の判断に關しての抛り所を与えることができる。

#### 【図面の簡単な説明】

【図1】実施形態のシステムの構成を示す図である。

【図2】実施形態の登録DB13のデータ構成を示す図である。

【図3】実施形態のHTMLファイル16のデータ構成を示す図である。

【図4】実施形態の登録者端末3のWebブラウザ15の処理の流れを示すフローチャートである。

【図5】実施形態の文書存在証明サーバ1のWebサーバプログラム12の登録処理の流れを示すフローチャートである。

【図6】実施形態の文書存在証明サーバ1のWebサーバプログラム12の削除処理の流れを示すフローチャートである。

【図7】実施形態の閲覧者端末4のWebブラウザ15の検証処理の流れを示すフローチャートである。

【図8】実施形態のコンテンツ17の表示例を示す図である。

【図9】実施形態の表示装置6上に表示される登録情報を示す図である。

【図10】実施形態の存在確認ページの表示例を示す図である。

【図11】実施形態の文書の存在を証明するメッセージの表示例を示す図である。

【図12】実施形態の参考URLと確認のためのリンクとを表示する例を示す図である。

#### 【符号の説明】

1・・・文書存在証明サーバ、3・・・登録者端末、4・・・閲覧者端末、12・・・Webサーバプログラム、13・・・登録DB、14・・・ハッシュ、15・・・Webブラウザ、16・・・HTMLファイル、17・・・コンテンツ

【図2】

図2

図2: 登録DB

| 登録日付   | メールアドレス    | 文書URL               | ハッシュURL        |
|--------|------------|---------------------|----------------|
| 970707 | xxx@yyy.zz | http://www.xxx.yyy/ | http://hbb.yy/ |
| ...    | ...        | ...                 | ...            |

【図3】

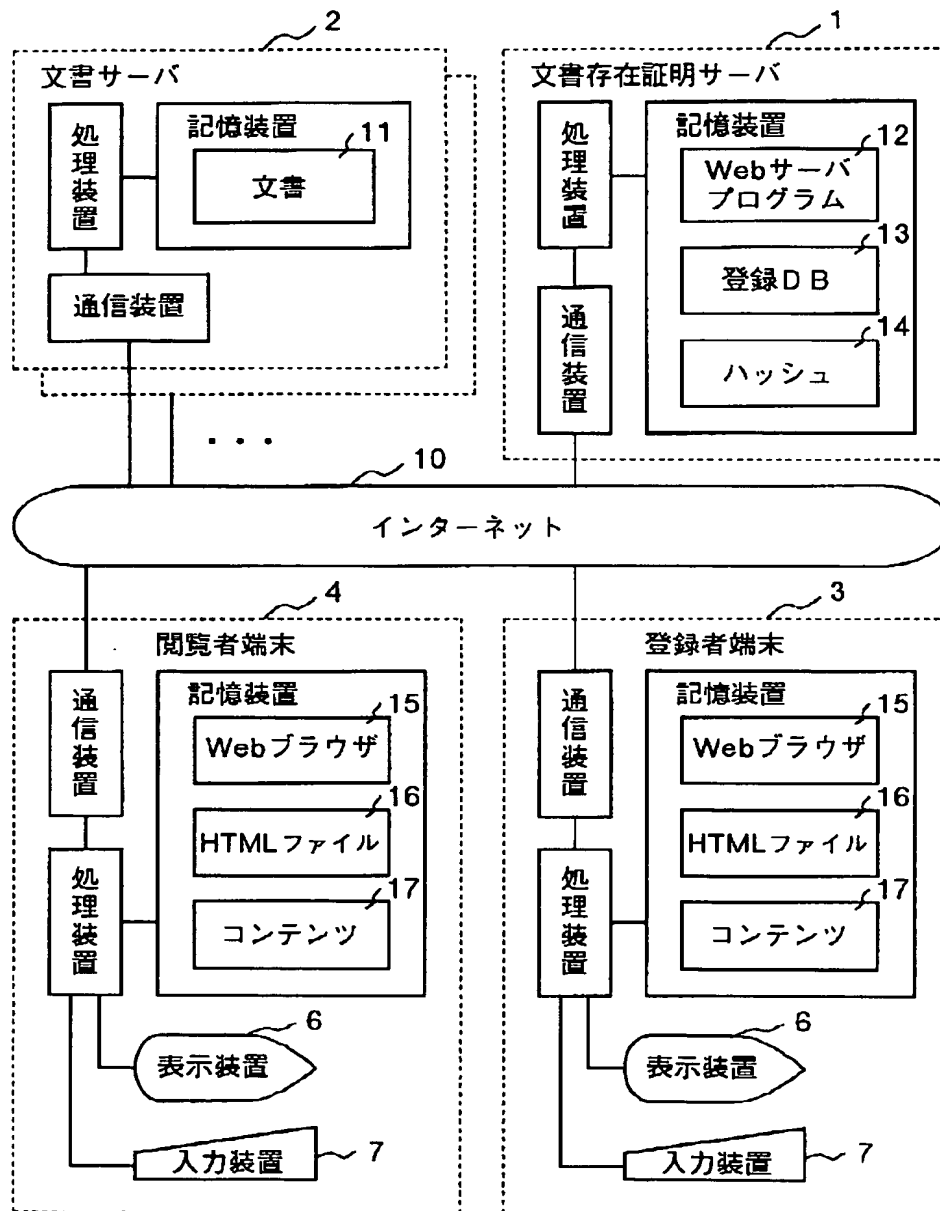
図3

図3: HTMLファイル

|                       |
|-----------------------|
| ・登録日付                 |
| ・コンテンツの元の存在場所を示すURL   |
| ・ローカルに保存されるコンテンツへのリンク |
| ・存在証明サーバのハッシュURL      |

【図1】

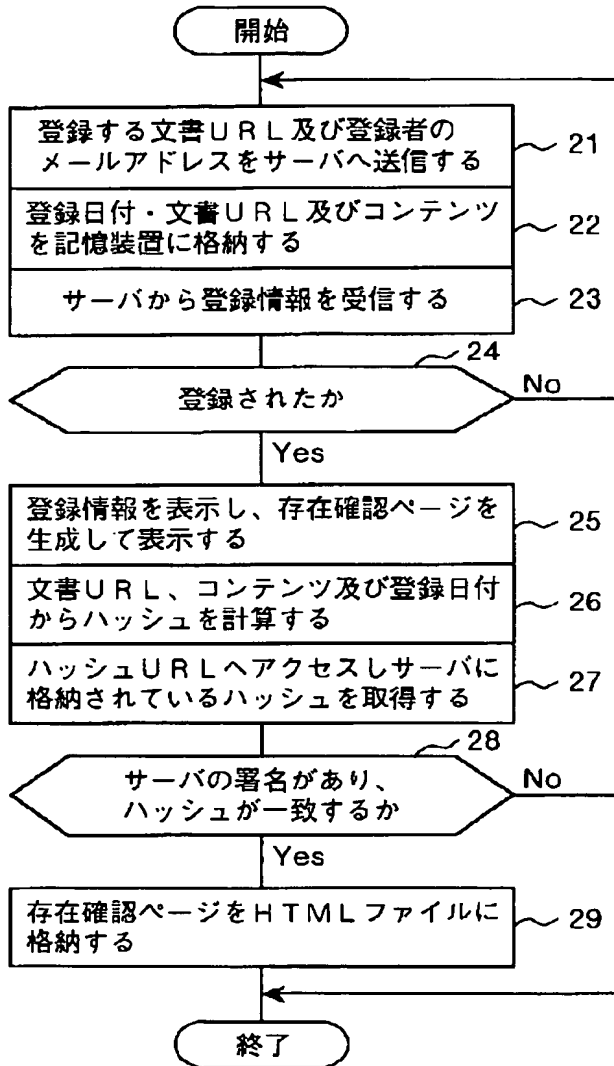
図 1





【図4】

図 4



【図8】

図 8

登録 検証

<http://www.xxx.yyy/>

WWW社、地銀と電子商取引の  
共同実験を開始

oooooooooooooooooooo  
oooooooooooooooooooo  
oooooooooooooooooooo  
oooooooooooooooooooo  
oooooooooooo

本ページを文書存在証明サーバへ登録  
することを認める。

E!'@'&'90!S", '80!G' &4' ('W' &@(' <PU!  
"!90!S

【図9】

図 9

登録 検証

登録情報

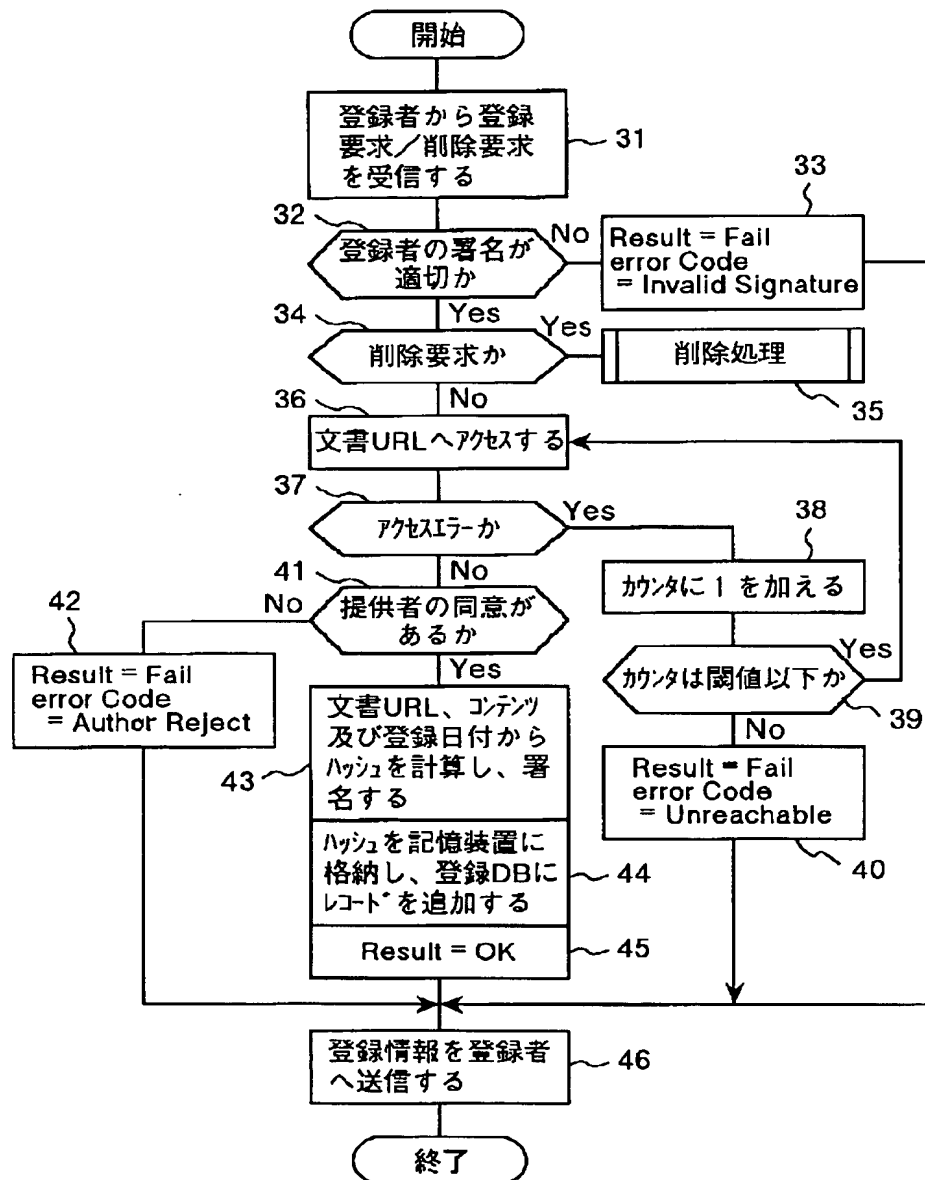
登録日付 19970707

文書URL <http://www.xxx.yyy/>

ハッシュ ハッシュへのリンク

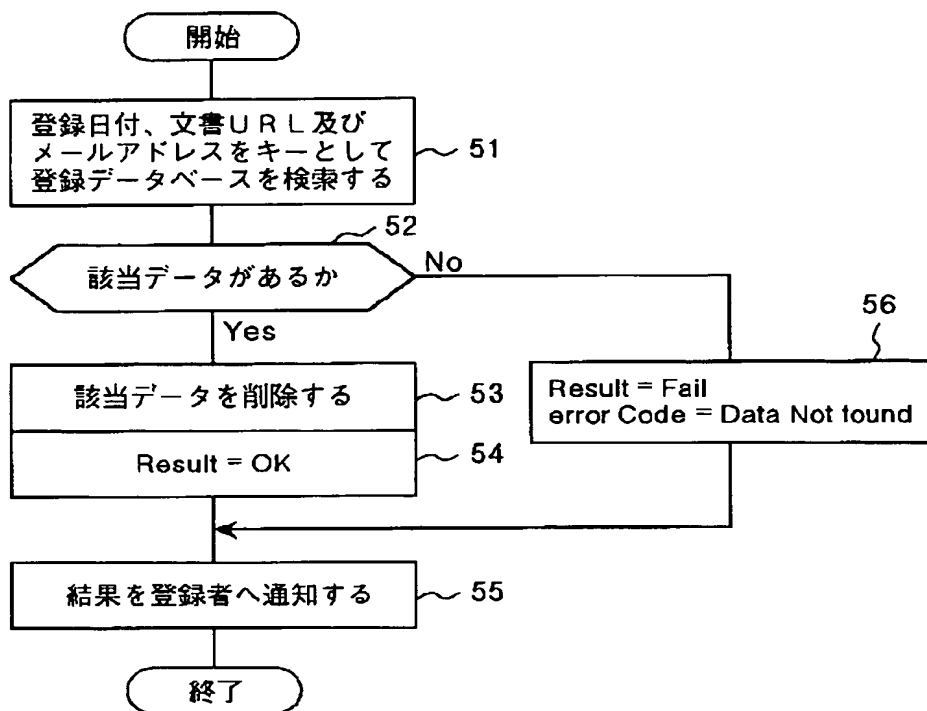
【図5】

図 5



【例 6】

☒ 6



【☒ 1 0】

10

【☒ 1 1】

111

【例 12】

12

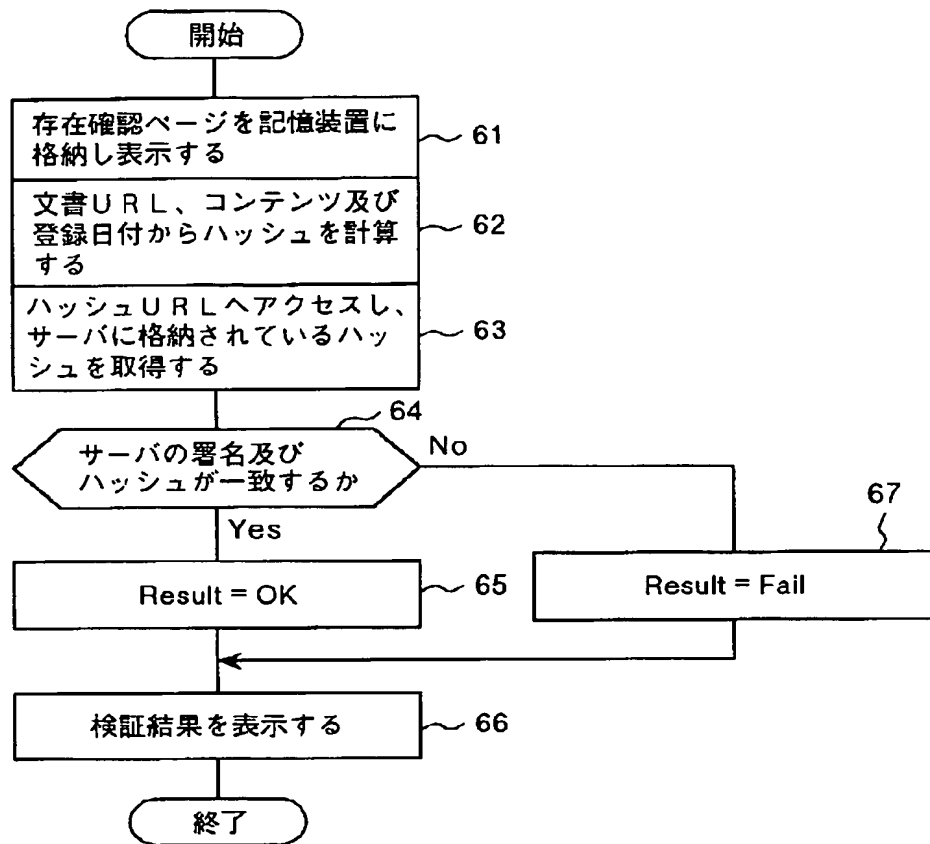
|                      |   |
|----------------------|---|
| 登録                   | 検証  |
| <input type="text"/> |   |
| 存在確認ページ              |   |
| 登録日付                 | 19970707  |
| 文書URL                | <a href="http://www.xxx.yyy/">http://www.xxx.yyy/</a> |
| ハッシュ                 | ハッシュへのリンク   |
| コンテンツ                | コンテンツへのリンク  |

|  |   |
|--|---|
| 登録   | 検証  |
| <input type="text"/>   |   |
| 存在確認ページ  |   |
| 登録日付   | 19970707  |
| 文書URL  | <a href="http://www.xxx.yyy/">http://www.xxx.yyy/</a> |
| 当該コンテンツは、19970707に<br><a href="http://www.xxx.yyy/">http://www.xxx.yyy/</a> に存在したことが確認されました。 |   |

|   |                                   |
|---|-----------------------------------|
| <input type="button" value="登録"/>   | <input type="button" value="検証"/> |
| <input type="text"/>  |                                   |
| <p style="text-align: center;">参考URL</p> <ul style="list-style-type: none"> <li>・ WWW社、地銀と電子商取引の<br/>共同実験を開始      ...<a href="#">確認</a></li> <li>URL http://www.xxx.yyy/<br/>○○○○○○○○○○○○○○○○○</li> <li>URL http://www.yyy.xxx.zzz/-bbb/      ...<a href="#">確認</a></li> <li>・ ××××××××××××××××</li> <li>URL http://www.zzz.yyy.xxx/-ccc/      ...<a href="#">確認</a></li> </ul> |                                   |

【図 7】

図 7



フロントページの続き

(72)発明者 富山 朋哉  
神奈川県横浜市都筑区加賀原二丁目2番  
株式会社日立製作所ビジネスシステム開発  
センタ内

(72)発明者 川連 嘉晃  
神奈川県横浜市都筑区加賀原二丁目2番  
株式会社日立製作所ビジネスシステム開発  
センタ内